IDENTITY-BASED RANDOM KEY PREDISTRIBUTION FOR ARMY MANETS

D. W. Carman
McAfee Research
Rockville, MD 20850

G. H. Cirincione
Army Research Laboratory
Adelphi, MD 20783

ABSTRACT[1]

We address a challenge to developing the Future Force — Army tactical networks require cryptographic keys to implement security services such as encryption and authentication, but current pairwise key establishment approaches using interactive public key techniques are too time-consuming. This paper describes identity-based cryptographic solutions that enable strong security and significantly reduce bandwidth consumption and latency, and provides three main contributions: (a) a description of how identity-based random key predistribution (IBRKP) can be used as a secure and efficient component within an Army tactical mobile ad hoc network (MANET) key management infrastructure; (b) a description of an attack on IBRKP resulting from *targeted* node compromises as opposed to *random* node compromises; and (c) a technique that creates "grainy" pool keys that increases security against targeted and random node compromise attacks.

1. INTRODUCTION

The Army of the future will rely on a heterogeneous mixture of networked combat elements to provide dominant situational understanding. Networked communications will often require multiple transmissions, or *hops*, to share data between sources and destinations. Operational tempo dictates these multi-hop communications occur rapidly—with little or no session set-up latency. Conventional key management techniques, such as Internet Key Exchange (IKE) and High Assurance Internet Protocol Encryption (HAIPE), require multiple time-consuming exchanges of public key information to establish security associations. When the cost of multiple exchanges is compounded over multiple hops, these conventional techniques may take precious seconds (or longer) to establish secure communications—failing to satisfy many basic operational scenarios.

2. IDENTITY-BASED RANDOM KEY PREDISTRIBUTION

Non-interactive key management techniques that rely on identity-based cryptography are a viable alternative that eliminates the costly public key exchanges of conventional techniques. These schemes leverage identities broadcast by MANET routing control messages to establish security associations **without exchanging any additional information**. We previously identified that reducing key management communications and latency was critical to enabling secure Army networks, and described how identity-based techniques could be used to efficiently key even resource-limited Army sensor networks [Carman et al., 2002]. However, existing identity-based public-key-based schemes are based on mathematical problems not yet accepted as "hard", and thus lack the maturity of cryptanalytic review necessary for military use. Previously described interactive random key predistribution schemes [Eschenauer and Gligor, 2002][Chan et al., 2003] leverage probabilistic techniques to offer provably secure schemes, but require significant delays to establish a pairwise key.

More recently, practical non-interactive alternatives for establishing keys in MANETs have been introduced [Zhu et al., 2003][Di Pietro et al., 2003]. We call these schemes *identity-based random key predistribution*, since they provide the mechanisms and provable security of random key predistribution with identity-based derivation of pairwise keys. The IBKRP system consists of four stages: (1) a Key Authority securely generates a key pool; (2) the Key Authority distributes to nodes an identity-derived subset of the key pool called a *keyring*; (3) when establishing a security association, system nodes determine the intersection of each other's keyrings; and (4) nodes use this common key set to derive encryption and message authentication keys.

IBRKP can be integrated into the military key management infrastructure (KMI) by identifying a subset of Army tactical nodes with an "IBRKP-capable" *attribute*. Embedding this attribute into IBRKP-capable node identities allows nodes to use IBRKP to establish security associations when both communicants are capable, and to fallback and use slower (but interoperable) conventional KMI techniques when either

[1] Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011. The U. S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **00 DEC 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE

Identity-Based Random Key Predistribution For Army Manets

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

McAfee Research Rockville, MD 20850; Army Research Laboratory Adelphi, MD 20783

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**2**	

or both are not. Since presumably the vast majority of high-tempo Army MANET communications would be between IBRKP-capable MANET nodes, infrequent conventional KMI use will have little deleterious effect on MANET bandwidth. Military-relevant security levels can be achieved using conventional embedded CPUs and for large yet feasible keyring sizes (e.g., 2Mbytes). Moreover, as future computational and storage capabilities increase, IBRKP security will correspondingly increase. The IBRKP Key Authority is similar to a conventional Central Facility (CF) in today's Electronic Key Management System (EKMS), so benign fill of nodes by COMSEC custodians using a conventional KMI could be performed.

We implemented and successfully demonstrated IBRKP-based pairwise keying within a secure multi-hop connected platoon at the Fort Benning, GA Military Operations on Urban Terrain (MOUT) site. For the 2Mbyte keyring sizes of this prototype solution, we established pairwise keys in 26.5 milliseconds on a Pentium4 1.6 GHz laptop, as compared to the 55 milliseconds needed for a corresponding 2048-bit Diffie-Hellman public key operation with a 256-bit exponent.

3. SECURITY

We identify an attack unique to IBRKP that must be addressed before military use can be considered. A targeted attack consists of an adversary compromising a smaller set of t nodes out of a total set of n network nodes that *can* be compromised. If an adversary can derive all the key identifiers each node possesses, it can determine which set of t nodes will provide the complete set of keys it needs. When the number of nodes targeted for compromise is much less than the number of common keys, the probability an adversary's targeted compromise attack is only marginally better than a random compromise node attack. However, when the number of nodes targeted for compromise exceeds the number of keys in common, we observe that we have "excess" targeted compromise nodes. This excess is caused by the fact that there is no need to compromise a node if we do not obtain at least one new key that we need out of the targeted common pairwise key set. Thus, an adversary need not target the compromise of more than i nodes, even when capable of doing so. Therefore, the probability of a successful attack is the same over the range $i < t \leq n$, and is equal to $\left(1-(1-m/S)^n\right)^i$, where m is each node's keyring size, and S is the key pool size.

Our most promising strategy for mitigating this attack is by increasing the number of common keys through the use of grainy pool keys. The grainy pool keys approach increases overall security by reducing each pool key's size, allowing each node to possess more keys, thus increasing the number shared by each pair. Although an adversary need not obtain the entire common key set to break a pairwise link, Fig. 1 illustrates the security benefits when using a 2MByte keyring size and a constant keyring size to pool size ratio for key sizes of 8, 64, and 256-bits. For the 2^{-256} probability of compromise metric, the 8-bit key method resists more than 1400 random node compromises, while the 256-bit key method resists less than 250. A drawback of the grainy approach is that for the same overall keyring size, computing common key sets takes longer and consumes more temporary memory due to the increased number of keys.

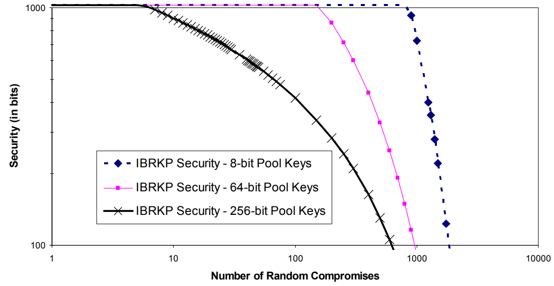

Fig. 1 – Resistance to Random Node Compromises

CONCLUSION

We have addressed an Army need to rapidly establish MANET security associations by describing a provably secure identity-based random key predistribution system that can be integrated into the Army KMI. We further described how our grainy pool key approach further strengthens this technology for military use.[2]

REFERENCES

Carman, D., Matt, B., and Cirincione, G., Energy-efficient and low-latency key management for sensor networks, Proceedings of the 23rd Army Science Conference, Dec 2002.

Chan, H., Perrig, A., and Song, D., Random key predistribution schemes for sensor networks, IEEE Symposium on Security and Privacy, May 2003.

Di Pietro, R., Mancini, L., and Mei, A., Random key-assignment for secure wireless sensor networks, SASN '03, Oct 2003.

Eschenauer, L. and Gligor, V., A key-management scheme for distributed sensor networks, Proceedings of the Ninth ACM Conference on Computer and Communications Security, Nov 2002.

Zhu, S., Xu, S., Setia, S., and Jajodia, S., Establishing pair-wise keys for secure communication in ad hoc networks: a probabilistic approach, 11th IEEE International Conference on Network Protocols, 2003.

[2] The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U. S. Government.